イントラネットにおける非ユーザ主導型通信の観測に関する研究

東北工業大学地域連携センター・研究支援センター紀要 EOS
Vol.34 No.1 p.33 ～ p.38, 2021

令和２年度学内公募研究（萌芽型）
〔技術報告〕

イントラネットにおける 非ユーザ主導型通信の観測に関する研究

角田　　裕 [1)]，樽川　正勝 [2)]，本多　善貴 [2)]

A study for monitoring of non-user-initiated traffic in intranets

Hiroshi TSUNODA [1)], Masakatsu TARUKAWA [2)], Yoshiki HONDA [2)]

Abstract

A complete understanding of network traffic sent and received by intranet hosts is the ultimate goal for intranet security management. However, network forensics against the massive amount and a wide variety of traffic is complex, and thus we need to prioritize the targeted traffic for the forensics. In particular, it is crucial to be aware of network traffic that a user does not directly initiate because such non-user-initiated traffic might be caused by any malicious element such as malware. This study gives two contributions: 1) developing the monitoring mechanism of non-user-initiated traffic toward unused IP addresses in IPv6 network and 2) demonstrating the host-wise analysis of non-user-initiated traffic in a real-operated intranet.

１　はじめに

イントラネット（組織内ネットワーク）を流れるあらゆる通信の完全な理解は，イントラネットセキュリティ管理上の理想である。しかし，膨大かつ多様な通信のすべての精査は困難であることから現状は理想には程遠く，効率的なネットワークフォレンジクス（ネットワーク上の科学捜査）のための技術開発が求められている。そこで本研究では，まずOSやソフトウェアがユーザの操作とは無関係に行う「非ユーザ主導型通信」に着目して，その実態を明らかにするために非ユーザ主導型通信の観測機構に関する研究を実施したので報告する。以下２.では今後の普及が予想されるIPv6を利用したイントラネットにおいて，未使用IPアドレス宛のパケットを観測する機構について説明する。また，３.では，ホスト単位のトラフィック監視機構を構築し，非ユーザ主導型通信を観測・分析して得ら

１）東北工業大学　工学部　情報通信工学科
Department of Information and Communication Engineering, Faculty of Engineering, Tohoku Institute of Technology
２）東北工業大学　工学部　情報通信工学科（令和３年３月卒業）
Department of Information and Communication Engineering, Faculty of Engineering, Tohoku Institute of Technology（Graduated in March 2021）

れた知見について報告する。

2　IPv6 イントラネットにおける未使用 IP アドレス宛パケットの観測

イントラネットにおいて利用可能な IP アドレスがすべて実際に使用されているわけではない。例えば，一般に家庭のホームネットワークのような小規模のイントラネットでは 254 個の IP アドレスが利用可能だが，そのうち実際に使用されているアドレスは 10 個を下回るような例は珍しくなく，多数の IP アドレスが未使用のままとなっている。このような未使用 IP アドレス宛にユーザが意図的に通信を行うことは通常ありえないため，そのような通信は非ユーザ主導型の通信で，かつマルウェアの感染活動などの何らかの異常によるものであり，優先的にフォレンジクス対象とすべきといえる。本研究室で，今後普及が予想される IPv6 を採用したイントラネットを想定し，未使用の IP アドレスに送信されるパケットの観測機構を検討・提案し，プロトタイプ実装を行った。なお，本成果は文献［1］として学会発表を行っている。

2．1　未使用 IPv6 アドレス宛パケットの観測手法

未使用 IP アドレス宛パケットの観測には，ネットワークでの宛先 MAC アドレス解決の仕組みを利用する。宛先 MAC アドレス解決の流れを図 1 に示す。

まず，ホスト H_A は H_B の IP アドレスを解決対象としたパケットをブロードキャストする（図 1 ①）。このパケットは H_C にも届く。H_B は，自分の MAC アドレスを設定したパケットをユニキャストで H_A に返信する（図 1 ②）ことで，H_B の IP アドレスと MAC アドレスが紐づけられる。この解決された IP アドレスと MAC アドレスの情報はキャッシュとして H_A 上に保存される。以降 H_A はキャッシュに保存された情報を元に H_B へパケットを送ることができる。この MAC アドレス解決は IPv6 では Neighbor Discovery Protocol（NDP）［2］で実現され，①のパケットとして近隣要請（Neighbor Solicitation：NS）メッセージが，②のパケットとして近隣広告（Neighbor Advertisement：NA）メッセージが使用される。

図 2 に本研究で提案する IPv6 での未使用 IP アドレス宛パケット観測の流れを示す。本研究では，未使用 IP アドレスを解決対象とした NS メッセージ（図 2 ①）に対して，観測ホストの MAC アドレスを設定した NA メッセージを代理で返信（図 2 ②）することで，未使用 IP アドレス宛パケットの観測を実現する。

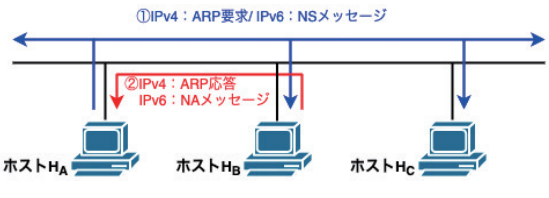

図 1　MAC アドレス解決の流れ

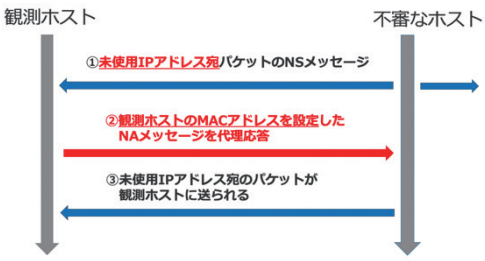

図 2　未使用アドレス宛パケットの観測方式

未使用 IP アドレス宛の NS メッセージに応答するホストは本来存在しない。しかし，観測ホストが代理で自身の MAC アドレスを設定した NA メッセージを返すことで，不審

なホストのキャッシュは未使用 IP アドレスと観測ホストの MAC アドレスが紐付けられる。従って，以降未使用 IP アドレス宛パケットは観測ホストに送信されるため，そこで観測できる。

観測における工夫として，パケットの宛先 IP アドレスが使用中か未使用かの判断方法がある。IPv4 では，サブネット内全ての IP アドレスに対して ping を送ることで使用中の IP アドレスを把握するが，IPv6 ではアドレス範囲が非常に広く，IPv4 同様の手法は現実的では無い。そこで IPv6 では，NS メッセージを観測した場合，観測ホストでもその解決対象の IP アドレスに NS メッセージを送信し，応答があった IP アドレスを使用中とする。応答が無かった IP アドレスは，未使用と判断し，観測ホストが代理で NA メッセージを返信する。

2．3　実装と観測実験

Python のパケット生成ライブラリ Scapy を使用して提案手法を実装し，研究室内のネットワークで未使用 IPv6 アドレス宛パケットの観測実験を行なった。ネットワークには，約 20 台のホストが接続されており，そこに観測手法を実装した観測ホスト，不審なホストに見立てた各 1 台を接続して行った。不審なホストが ping コマンドを用いて未使用 v6 アドレス宛に 50 個の Echo request パケットを送信した。

図 3 に，不審なホストから未使用の IP アドレス fe80::9789:50d8:4b01:eeee 宛に ping を実行した際に観測ホストが観測したパケットを示す。①が不審なホストが送信した未使用 IP アドレスを解決対象とした NS メッセージ，②がそれに対して観測ホストがその IP アドレスが使用中かを確認する為に送信した NS メッセージである。これに対する応答が無かった為，③で観測ホストが代理 NA 応答を不審なホストに対して返信している。この結果，未使用 IP アドレス宛の Echo request が観測ホストに向けて送信されるため，赤枠部分に示すように観測に成功していることがわかる。

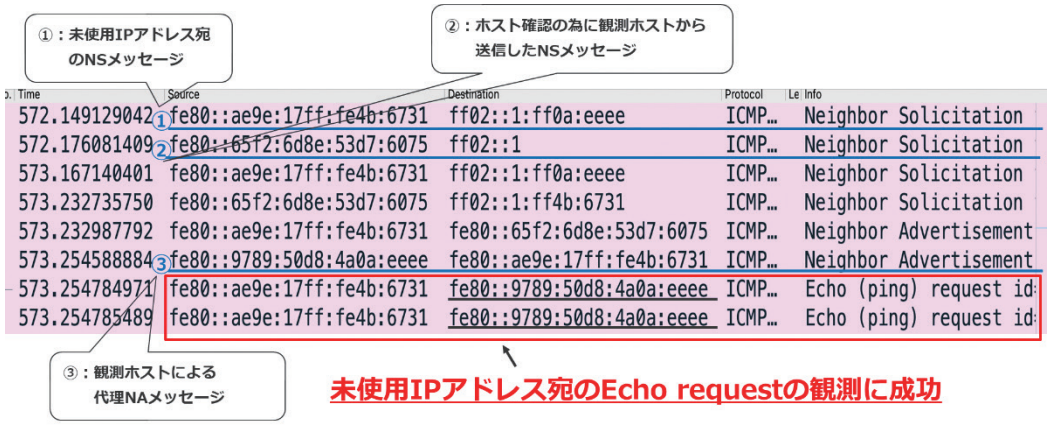

図 3　未使用 IPv6 アドレス宛パケットの観測実験の結果

3　ホスト単位の非ユーザ主導型通信の調査

前節で提案した機構では，未使用 IP アドレス宛以外の非ユーザ主導型通信は観測できない。そこで，ホスト毎の通信とログ（動作履歴情報）を観測・収集して一元管理する体

制を整備し，観測実験を実施した。実験では，Windows 10 のホストの通信を 24 時間継続監視し，その中からログの情報に基づいて非ユーザ主導型通信のトラフィックのみを抽出・分析した。具体的には，ホストのログからホストがスリープ状態にあった時間帯を特定し，その時間帯に発生した通信を非ユーザ主導型通信とみなして精査した。今回の実験で観測したイントラネット内外との通信は，すべて発生理由や原理が説明可能なもので，フォレンジクス対象から除外可能であることが確認できた。なお，本成果は文献［3］として学会発表を行っている。

3．1　観測実験の概要

観測実験のネットワーク構成図を図 4 に示す。非ユーザ主導型通信の観測対象は Windows 10 を搭載したホストであり，このホストが送受信するトラフィックをフラッディングスイッチで分流し Linux を搭載したホスト（以下，モニタ）で観測する。モニタが観測したトラフィックデータと，観測対象ホストの Windows イベントログは収集分析サーバに送信され，一元管理・分析の対象となる。モニタは管理用のセグメントを通じてサーバにトラフィックデータを送信し，ホストはサービス用セグメントを通じてイベントログをサーバに送信する。サーバでは，受信したイベントログのインスタンス ID に基づいて，ホストがスリープ状態にあった時間帯を判断し，その時間帯のトラフィックを非ユーザ主導型通信のトラフィックとみなして分析した。

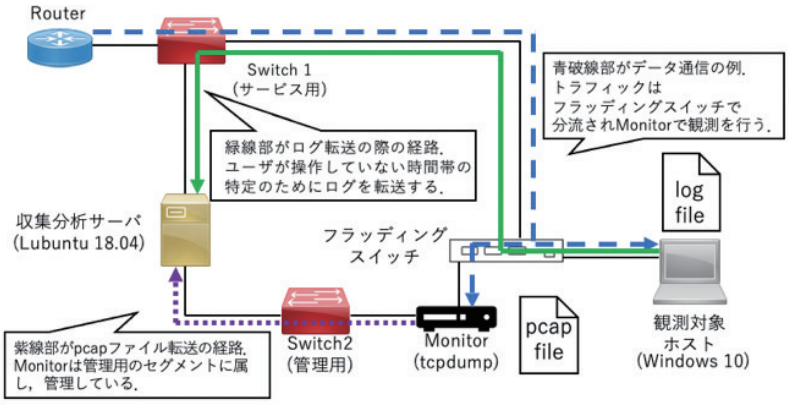

図 4　観測機構の構成

3．2　非ユーザ主導型通信の分析結果

2021 年 1 月 10 日から 12 日において，ホストが行った非ユーザ主導型通信により発生したパケットは合計 769 個であり，そのうち 457 パケットはネットワーク外との通信，312 パケットはネットワーク内での通信によるものだった。

ネットワーク外を宛先とする通信はすべて HTTP または HTTPS によるものだった。表 1 に，宛先のドメイン名とポート番号，またドメイン名の情報からマイクロソフトの公式ドキュメントに基づいて判断した通信の発生理由をまとめた。

ネットワーク内を宛先とする通信は 4 種類のプロトコルによるものであった。表 2 に，プロトコル毎の通信相手，各プロトコルの機能とパケットの内容から判断した通信の発生理由をまとめた。

表１　ネットワーク外との通信の調査結果

	通信相手	パケット数	通信の発生理由
（１）	settings-win.data.microsoft.com:443	147	最新の機能更新プログラムの取得などのため
（２）	edge.microsoft.com:443	73	Microsoft Edgeが新しい更新プログラムを確認するため
（３）	smartscreen-prod.microsoft.com:443	56	WindowsのSmart Screenサービスにおける URLの危険性の調査のため
（４）	ctldl.windowsupdate.com:80	51	ルート証明書の自動更新のため
（５）	v10.events.data.microsoft.com:443	44	診断データをマイクロソフトに送信するため
（６）	scrootca1.ocsp.secomtrust.net:80	30	TLS証明書の失効情報を取得するため，（６）は中間CA証明書，（７）はクロスルート用中間CA証明書の失効情報取得時の通信相手となる
（７）	scrootca2.ocsp.secomtrust.net:80	30	
（８）	tsfe.trafficshaping.dsp.mp.microsoft.com:443	26	Windows UpdateとMicrosoft Storeバックエンドサービスのために行われる通信

表２　ネットワーク内の通信の調査結果

プロトコル	通信相手	パケット数	通信の発生理由
SSDP（Simple Service Discovery Protocol）	マルチキャストアドレス	183	Windows 10が定期的に行うネットワーク上の機器を自動的に発見・接続する動作のため
DNS（Domain Name System）	DNSサーバ	72	ネットワーク外の通信先と通信する際の名前解決のため
ICMP（Internet Control Message Protocol）	デフォルトルータ	48	デフォルトルータへの接続性を確認するため
BROWSER	マルチキャストアドレス	9	ネットワーク上のコンピュータ名の一覧を維持・管理するため

２つの表からわかるように，今回の実験で観測した非ユーザ主導型通信はすべて発生理由や原理が説明可能なものだった。つまり，これらの通信はフォレンジクス対象からは除外可能である。今後，このような調査を継続的に実施し，フォレンジクス対象外とできる通信の宛先の情報を蓄積することで，フォレンジクスの作業を効率化できる可能性がある。

４　今後の課題

本研究では，イントラネットにおけるネットワークフォレンジクスの効率化を目指し，非ユーザ主導型通信に焦点を絞って観測機構を検討し，観測した通信トラフィックの分析を行った。IPv6イントラネットにおける未使用IPアドレスに対する非ユーザ主導型通信の観測については，実運用IPv6イントラネットにおける実証実験が必要である。一方，ホスト単位の非ユーザ主導型通信の観測については，観測対象ホストの台数や種別を増やして継続的な観測を行い，フォレンジクス対象からは除外可能なトラフィックの情報を蓄積することが課題である。

謝辞

本研究は，東北工業学内公募研究（2020-04）の援助により行われたものである。ここに記して謝意を表する。

参考文献

［1］本多善貴，角田裕，“IPv6 イントラネットにおける未使用 IP アドレス宛パケットの観測”，令和３年東北地区若手研究者研究発表会 R3-E-17，2021 年３月
［2］Thomas Narten,”Neighbor Discovery for IP version 6（IPv6）”，RFC4861，Sept. 2007
［3］樽川正勝，角田裕，“イントラネットにおけるホスト単位の通信監視の試行”，令和３年東北地区若手研究者研究発表会 R3-E-18，2021 年３月